AFFIDAVIT OF SPECIAL AGENT EUGENE WHEELIS IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, EUGENE WHEELIS, having been sworn, state:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent employed by the Diplomatic Security Service ("DSS") of the United States Department of State. I have been employed as a Special Agent with DSS for approximately 2 years. I am authorized to make arrests for violations of federal law.

2. I am currently investigating Yris SANCHEZ, *a/k/a* Yolanda GOMEZ VELEZ, for aggravated identity fraud in violation of 18 U.S.C. § 1028A, fraudulent use of a U.S. passport in violation of 18 U.S.C. § 1544, and misuse of a Social Security number in violation of 42 U.S.C. § 408(a)(7)(B) (the "Target Offenses"), and for other federal criminal violations.

3. This affidavit is being submitted in support of an application for a warrant, under 18 U.S.C. § 2703(a) and Rule 41 of the Federal Rules of Criminal Procedure, to search and seize the Facebook account identified by the URL www.facebook.com/yris.sanchez and other data associated with this account ("the SANCHEZ Facebook Account"), as described in Attachment A. There is probable cause to believe that the SANCHEZ Facebook Account contains fruits, evidence, and instrumentalities of the Target Offenses, as described in Attachment B.

4. The SANCHEZ Facebook Account and relevant data is maintained by Facebook, Inc., which, government databases indicate, accepts service of process at 1601 Willow Road, Menlo Park, CA 94025 and via its law enforcement portal at www.facebook.com/records.

5. The facts in this affidavit come from my personal observations and review of records, my training and experience, and information obtained from other agents and witnesses. This affidavit includes only those facts I believe are necessary to establish probable cause and does not include all of the facts uncovered during the investigation.

FACEBOOK

6. Facebook is an online social networking service accessible at the website www.facebook.com or via an application ("app") that can be installed on computer equipment, including a tablet or a cell phone. Facebook allows users to create profiles and share personal and biographical information; share content and media, including by uploading photographs and videos and sending links to other content; and communicate with other users in a variety of ways, from public discussions to private messaging.

7. When a user creates a Facebook account, he or she provides Facebook with information to begin building their online Facebook profile, including uploading at least one photo and selecting a Vanity Name and email address that will be associated with the account. The user may choose to provide other information as well for the "About Me" section of the page, including basic information such as where the user lives, works, and attends/attended school. This information is then displayed on the user's page. The user may also provide Facebook with other contact information, such as phone numbers and email addresses. In addition, Facebook captures certain basic information about the new account, including the registration date and the IP address used to create the account. Further, Facebook assigns a unique numerical identifier to the account.

8. Facebook users can continually build their online profile, and in my training and experience it is common for users to add and edit biographical information – for instance by updating on a new job or changing a "relationship status" to reflect changes in their life. Facebook actively prompts users to provide or confirm information, for instance by asking the user to confirm that they live in a particular city if other information in the profile or the majority of connections suggests that they might live in that city. As a result, Facebook users often provide a significant amount of biographical information.

9. Facebook also encourages users to form connections with other users on the site, most fundamentally by allowing users to connect as "Friends." A Facebook user creates a "Friend" connection by inviting another Facebook user to confirm that they are "Friends." When the request is accepted, the connection is created. Facebook also prompts users to connect with other users when they share common connections.

10. Facebook offers users a variety of privacy settings. The Vanity Name and the Profile Picture and Cover Photo are publicly visible to anyone that visits the page, and are generally searchable unless a user has selected not to be searchable. Facebook users can keep their entire profile open publicly as well, which allows anyone to view all of the content and information on their profile. The Facebook can make the content of their page visible only to users that have been confirmed as "Friends," or visible to both "Friends" and anyone confirmed as a "Friend" of their "Friend" (exponentially increasing the number of people that can view that content). Further, Facebook users can create lists within their "Friends" and allow certain content to be viewed only by subgroups of their Friends (e.g. "Friends" designated as "Work Friends," or "Family").

11. The first page of every Facebook account displays a Vanity Name and the space for both a "Profile Picture" and a "Cover Photo." Facebook users can post additional photos or even entire photo albums. In my training and experience, most Facebook users build their profiles by uploading and changing photographs on their account. Many users own mobile devices that contain cameras, and it is common for mobile cameras and popular camera mobile applications (such as Instagram, an application owned by Facebook) to prompt users to post pictures to their Facebook accounts after a photo is taken.

12. Facebook users have the ability to indicate that other people who appear in their photos are also on Facebook by "tagging" them in the photograph using their Vanity Name. A Facebook user

can adjust their privacy settings to require that they confirm a tag before it can be successfully applied.

13. Facebook users can comment on their own photographs and other users' photographs or indicate that they "Like" a particular image.

14. In addition to photographs, Facebook users can write messages, or "Status Updates," on their page. This was traditionally referred to as their "wall" or a "wall post," and is now called a "Timeline." Unless the user actively deletes them, older postings may be viewable on the users' account by looking back through the "Timeline." Facebook users can also add "life events" with a date on their "Timeline," such as the date they began a particular job or were married. As with photographs and other content, the user can select who can view their posts – allowing them to be visible publicly (the default) or limiting their display to only a selected group of individuals.

15. Facebook users can also send private messages to other Facebook users, as well as to email addresses. These messages are only viewable by the recipient.

16. Facebook users can also create or join "Groups" of other users. Facebook Groups are used by a variety of communities and small groups and are a tool to communicate and share content.

17. Facebook also allows public figures, businesses, organizations, and other entities to create Facebook Pages. Facebook users can become "Fans" of a Facebook Page.

18. Facebook users provide information about their physical location in different ways through their use of Facebook. Depending on the user's privacy settings, Facebook may also obtain and store the physical location of the user's device(s) as they interact with the Facebook service on those device(s). As described above, Facebook users may also affirmatively state their current address and their hometown. Facebook users may also post Status Updates that discuss where they are, who they are with, and what they are doing. Facebook users who are using a mobile

device running the Facebook application may also be able to "Check In" to a location using a feature called "Facebook Places" if the location or establishment from which they are posting offers this feature. The check-in feature allows Facebook users to connect with other users, or "Friends," that are at or near the same location. In addition, Facebook collects other locational information regarding its users, such as the IP address for the device each time the user logs into the site.

19. While it is free to create a profile and use Facebook, Facebook does collect payment information for some uses. Companies that use Facebook can purchase advertisements and sponsored posts. Individual users can use Facebook Marketplace, an online classified service, to sell or purchase items. Facebook users can also purchase games and software applications, and related real or virtual products. Facebook users can also purchase "Facebook Credits" that can then be used for games and application purchases.

20. Facebook encourages connectivity and sharing, and numerous websites now allow users to access services or login to their pages through their Facebook account. In addition, many websites allow users to use Facebook to indicate that the user "Likes" the website, product, or affiliated group. Based on my training, I understand that Facebook also often obtains information regarding other internet activity by its users, even when that user has not actively logged in or affirmatively selected the "Like" button.

21. Facebook was founded in 2004 and has continually evolved, adding different types of services. In 2012, Facebook announced that it had grown to have more than 1 billion active users.

PROBABLE CAUSE THAT THE SANCHEZ FACEBOOK ACCOUNT CONTAINS FRUITS, EVIDENCE, OR INSTRUMENTALITIES OF THE TARGET OFFENSES

22. This investigation has established evidence that Yris SANCHEZ, a Dominican national, has fraudulently applied for and obtained a U.S. passport in the name of Yolanda GOMEZ VELEZ, a U.S. citizen born and living in Puerto Rico. Specifically, the State Department received the following applications in the SANCHEZ identity (collectively, the "Fraudulent Passport Applications"):

a. On October 3, 2005 form DS-11 (Application for a U.S. Passport) # 170011902 was executed at U.S. Post Office Harvard Square, Cambridge, MA. The individual applying for the passport listed her identity as Yolanda GOMEZ VELEZ, date of birth xx/xx/1977, with a Social Security number ("SSN") ending in 4172. As a result of this application, U.S. passport # 170011902 was issued.

b. On September 11, 2006, the same individual executed DS-11 # 309532274 at the Harvard Square Post Office, after reporting the previously issued passport as stolen. On this DS-11, the applicant again claimed the name Yolanda GOMEZ VELEZ with date of birth xx/xx/1977 and SSN ending in 4172. The photograph included with this application is of the same individual whose photograph appears on DS-11 # 170011902. As a result of this application, U.S. Passport # 309532274 was issued.

c. On June 9, 2016, form DS-82 (Passport Renewal Application) # 275443637 was mailed to the National Passport Center ("NPC") in Portsmouth, NH for processing. On this form, the applicant again claimed the name Yolanda GOMEZ VELEZ with date of birth xx/xx/1977 and SSN ending in 4172. Included with the DS-82 was passport # 309532274. The individual in the photograph included with

DS-82 # 275443637 strongly resembles the individual pictured in applications # 170011902 and # 309532274. As a result of this application, U.S. Passport 551722824 was issued.

23. An analysis of travel records within Customs and Border Protection ("CBP") databases showed that passport # 551722824 was used for frequent international travel between 2016 and 2019. Specifically:

a. On January 1, 2016 passport # 309532274 was presented to board United Airlines flight 1486 departing Newark, New Jersey ("EWR") en route to Gregorio Luperon International Airport, Puerto Plata, Dominican Republic ("POP"). The same passport was used on United Airlines flight 1484 returning from POP and landing at EWR on January 8, 2018.

b. On August 8, 2016 passport # 551722824 was presented to board American Airlines flight 1481 departing Miami International Airport ("MIA"), en route to Santo Domingo, Dominican Republic ("SDQ"). The same passport was used on American Airlines flight 1154 departing SDQ and landing at MIA on August 17, 2016.

c. On May 27, 2017 passport # 551722824 was presented to board JetBlue flight 923 departing Boston Logan Airport ("BOS") en route to Cibao International Airport, Santiago, Dominican Republic ("STI"). The same passport was used on JetBlue flight 924 returning from STI and landing at BOS on June 12, 2017.

d. On September 25, 2017 passport # 551722824 was presented to board JetBlue flight 1528 departing POP and landing at JFK International Airport ("JFK").

e. On November 26, 2018 passport # 551722824 was presented to board Delta flight 391 departing SDQ and landing at JFK.

f. On July 22, 2019 passport # 551722824 was presented to board JetBlue flight 129 departing BOS en route to SDQ. The same passport was used on JetBlue flight 830 returning from SDQ and landing at BOS on August 10, 2019.

24. On October 15, 2018, someone submitted an application for a "Real ID" driver's license to the Massachusetts Registry of Motor Vehicles ("RMV") in the name GOMEZ VELEZ. This application listed the SSN ending in 4172. The RMV photograph associated with this applicant depicts the same person who appears on the Fraudulent Passport Applications.

25. Diplomatic Security special agents have located and interviewed the true GOMEZ VELEZ, who confirmed that, while the biographical information present on the Fraudulent Passport Applications were her own, she did not submit these applications, and she was not the person depicted in the application photographs. During the interview, the true GOMEZ VELEZ confirmed that the SSN ending in 4172 was her own, and presented to the interviewing agents two separate Social Security cards bearing her name and that number.

26. Based on the foregoing, and on my training and experience, I believe that the Fraudulent Passport Applications and the October 2018 RMV application that were submitted under the GOMEZ VELEZ name were in fact fraudulently submitted by another person.

27. Furthermore, there is reason to believe that the user of the SANCHEZ Facebook Account is the person who has impersonated GOMEZ VELEZ and has committed the Target Offenses. Based on the facts reflected below, and on my training and experience, I believe that records associated with the SANCHEZ Facebook Account, including but not limited to photographs and evidence evincing the account's user, will constitute evidence of the Target Offenses.

28. The publicly-available profile photograph associated with the SANCHEZ Facebook Account depicts a photograph of a female who appears to be the same person depicted in the photographs associated with the Fraudulent Passport Applications and the 2018 RMV application. The name associated with the publicly-available profile of the SANCHEZ Facebook Account is Yolanda (Yris) SANCHEZ.[1]

29. Publicly-available information associated with the SANCHEZ Facebook Account show that the SANCHEZ Facebook Account has been posting photos, comments, and other content that establish a clear connection between the SANCHEZ Facebook Account and the Dominican Republic since at least 2013. Specifically, on August 31, 2013 the SANCHEZ Facebook Account made publicly available comments the Facebook profile of a Dominican national indicating an immediate family relationship with this individual. Additionally, on March 30, 2014, the SANCHEZ Facebook Account posted a photo of the account owner holding the flag of the Dominican Republic. The SANCHEZ Facebook Account has consistently posted similar content up to present day, including a photograph of SANCHEZ and the words "Orgullo Dominicano" superimposed on the image posted on February 27, 2019, which is also Dominican Independence Day.[2]

---

[1] As such, this affidavit will refer to the user of the SANCHEZ Facebook Account as "SANCHEZ." In my training and experience, identity fraudsters use social media to communicate with their friends and family with complete disregard for the integrity of their alias. In other words, identity criminals who are living in an alias will very often put their true name on their social media page, communicate with friends or family in a way that demonstrates a relationship that compromises an assumed identity, or, in some cases, brag or otherwise admit to conducting criminal behavior outright. I believe that the user of the SANCHEZ Facebook Account – even though she has obtained and used official identification documents under the GOMEZ VELEZ – has likely continued to use her true identity in connection with her Facebook account.

[2] While I am not a fluent speaker of Spanish, I understand that "Orgullo Dominicano" means "Dominican pride." In addition, SANCHEZ has made posts on several other Facebook users'

30. Furthermore, on the SANCHEZ Facebook Account, SANCHEZ lists herself as the owner of a Facebook business page called "HAIR BY YRIS", also known as "D'YRIS SALON." State Department records reveal that the fee for the passport application submitted on June 9, 2016 in the name of GOMEZ VELEZ was made via a check from a business account in the name of D'YRIS SALON.

31. Records maintained by Facebook concerning the SANCHEZ Facebook Account are likely to constitute evidence regarding the identity of the user of that account and/or the individual depicted in the account's profile photograph, including but not limited to evidence showing whether that user is the person who submitted the Fraudulent Passport Applications

32. On 09/09/2019, a request was submitted under 18 U.S.C. § 2703(f) via the Facebook law enforcement portal that the company preserve all records associated with the SANCHEZ Facebook Account. Facebook has indicated that it will preserve these records through 12/08/2019.

33. From my training and experience, I am aware that companies that host social-networking accounts, and Facebook in particular, generally maintain records of their subscribers' online activities and private communications unless the user deletes these communications.

---

pages indicating a familial connection. Using State Department databases, I confirmed that the apparent users of these other Facebook accounts are themselves Dominican nationals. In addition, a criminal search within the Treasury Enforcement Communications System ("TECS") using SANCHEZ's name and date of birth (as reflected in the publicly-available information regarding the SANCHEZ Facebook Account) produced a lengthy criminal record. Since 1992, SANCHEZ had been arrested for several fraud and theft felonies in both her true identity as well as two additional aliases. In the accompanying arrest reports SANCHEZ's nationality is listed as Dominican. Furthermore, CBP data available in TECS demonstrate that U.S. passport # 551722824 issued to Yolanda GOMEZ VELEZ was used to travel between the United States and the Dominican Republic at least ten times between 2016 and the present. This passport has not been used for any other international travel during the same period. I know, based on my training and experience, that individuals who submit fraudulent applications for U.S. passports are often foreign nationals seeking certain benefits associated with U.S. citizenship and/or seeking to travel between the United States and the country of their birth or citizenship.

LEGAL AUTHORITY

34. The government may obtain both electronic communications and subscriber information by obtaining a search warrant. 18 U.S.C. §§ 2703(a), 2703(c)(1)(A).

35. Any court with jurisdiction over the offense under investigation may issue a search warrant under 18 U.S.C. § 2703(a), regardless of the location of the Internet company whose information will be searched. 18 U.S.C. § 2703(b)(1)(A). Furthermore, unlike other search warrants, § 2703 warrants do not require an officer to be present for service or execution of the search warrant. 18 U.S.C. § 2703(g).

36. If the government obtains a search warrant, there is no requirement that either the government or the provider give notice to the subscriber. 18 U.S.C. §§ 2703(b)(1)(A), 2703(c)(3).

REQUEST TO SEAL AND PRECLUDE NOTICE TO THE SUBSCRIBER

37. I request that this application, the warrant, the order, and any related papers be sealed by the Court until such time as the Court directs otherwise, except that the United States may later produce copies of the search warrant and related documents to the defense during discovery in any criminal case.

38. I further request that, pursuant to the non-disclosure provisions of 18 U.S.C. §§ 2705(b), the Court order Facebook not to notify any person (including the subscribers or customers to which the materials relate) of the existence of this application, the warrant, the Order, or the execution of the warrant, for a period of one year from the date of this Order, or until notified by the government within thirty days of the conclusion of the investigation, whichever is earlier. Facebook may disclose this Order to an attorney for Facebook for the purposes of receiving legal advice.

39. Non-disclosure is appropriate in this case because the Court's order relates to an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation, and

its disclosure may alert the targets to the existence of the investigation. There is accordingly reason to believe that notification of the existence of the Order will seriously jeopardize the investigation by: giving targets an opportunity to flee or continue flight from prosecution, destroy or tamper with evidence, or change patterns of behavior. See 18 U.S.C. § 2705(b). Moreover, some of the evidence in this investigation is stored electronically. If alerted to the existence of the Order, the targets could destroy that evidence, including information saved to their personal computers, on other electronic media, or in social media accounts.

FOURTEEN-DAY RULE FOR EXECUTION OF THE WARRANT

40. Federal Rule of Criminal Procedure 41(e)(2)(A),(B) directs the United States to execute a search warrant for electronic evidence within 14 days of the warrant's issuance. If the Court issues this warrant, the United States will execute it not by entering the premises of Facebook, as with a conventional warrant, but rather by serving a copy of the warrant on the companies and awaiting their production of the requested data. This practice is approved in 18 U.S.C. § 2703(g), and it is generally a prudent one because it minimizes the government's intrusion onto Internet companies' physical premises and the resulting disruption of their business practices.

41. Based on the training and experience of myself and other law enforcement, I understand that e-mail and social media providers sometimes produce data in response to a search warrant outside the 14-day (formerly 10-day) period set forth in Rule 41 for execution of a warrant. I also understand that electronic communication companies sometimes produce data that was created or received after this 14-day deadline ("late-created data"). The United States does not ask for this extra data or participate in its production.

42. Should Facebook produce late-created data in response to this warrant, law enforcement personnel will seek to avoid reviewing any late-created data that was created by or received by the

account-holder(s) absent a follow-up warrant. However, I request permission to view all late-created data that was created by Facebook, including subscriber, IP address, logging, and other transactional data, without a further order of the Court. This information could also be obtained by grand jury subpoena or an order under 18 U.S.C. § 2703(d), neither of which contains a 14-day time limit.

43. For these reasons, I request that the Court approve the procedures in the respective Attachments B, which set forth these limitations.

CONCLUSION

44. Based on the information described above, I have probable cause to believe that Yris SANCHEZ has committed aggravated identity fraud and fraudulent use of a U.S. passport, in violation of 18 U.S.C. § 1028A and 1544.

45. Based on the information described above, there is probable cause to believe that the SANCHEZ Facebook Account (as described in Attachment A) contains fruits, evidence, and instrumentalities of these crimes (as described in Attachment B).

46. The procedures for copying and reviewing the relevant records are set out in Attachment B.

Sworn to under the pains and penalties of perjury

Special Agent Eugene Wheelis
Diplomatic Security Service

Sworn to and subscribed before me

Dated: October 18, 2019

Honorable M. Page Kelley
United Sates Magistrate Judge